IN THE UNITED STATES COURT OF FEDERAL CLAIMS
BID PROTEST

AMAZON WEB SERVICES, INC.

Plaintiff,

v.

THE UNITED STATES,

Defendant,

and

MICROSOFT CORPORATION,

Intervenor-Defendant.

Final Redacted Version

Case No. 19-1796

Judge Patricia E. Campbell-Smith

[redacted]

INTERVENOR-DEFENDANT'S MEMORANDUM IN OPPOSITION TO PLAINTIFF'S MOTION FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

[redacted]

TABLE OF CONTENTS

[redacted]

[redacted]

TABLE OF AUTHORITIES

Page(s)

CASES

[redacted]

[redacted]

STATUTES

OTHER AUTHORITIES

[redacted]

INTRODUCTION

Amazon Web Services, Inc. (AWS) comes to this Court seeking emergency injunctive relief to stop the Department of Defense (DoD) from launching its critical Joint Enterprise Defense Infrastructure (JEDI) Cloud project. But it does so *three months* after the JEDI contract was awarded to Microsoft and *two months* after AWS filed its complaint. AWS offers no excuse for its delay in filing this motion, which is not based on any new information or change in DoD's timeline. Instead, AWS seeks to enjoin performance of the contract that has been planned for months—and that is critical to national security—based almost entirely on information it knew at the time it filed its complaint. AWS's delay weighs heavily against granting that request.

AWS's motion also fails on substance. Notably, AWS does not even try to defend the bias and conflict of interest allegations that take up dozens of pages and three counts of its complaint. AWS filed this case with great fanfare, claiming that a series of colorful statements from President Trump directly influenced the decisions of dozens of technical and procurement experts at DoD. But the administrative record contains *nothing* to substantiate this baseless criticism. AWS's decision to ignore its bias claims confirms those claims have no likelihood of success on the merits. And AWS also ignores many of the complaint's more technical challenges to the award, including all of Count III. For the purposes of this motion, AWS has abandoned half its case.

Instead, AWS tries to justify its request for injunctive relief by second-guessing DoD's expert judgment regarding its own needs and minimizing the fundamental national security interests at stake in a quick and orderly ramp-up of the JEDI Cloud. But AWS fails to establish its entitlement to a preliminary injunction under any of the four traditional factors.

First, AWS hinges its likelihood of success on the merits on a series of alleged technical errors in the evaluation that are, at best, mere disagreements with the agency's conclusions, and,

[redacted]

at worst, inaccurate representations of DoD's criteria and the offerors' proposals. None of AWS's challenges to the expertise and judgment of the DoD evaluators has merit, much less supports their request for extraordinary injunctive relief.

Second, AWS has not established irreparable harm of any kind. AWS insists that it is being deprived of the opportunity to compete for the JEDI contract, but it fails to tie that harm to its need for a preliminary, rather than permanent, injunction. Its speculative contention that Microsoft will gain a competitive advantage in any recompete has no merit.

Third, AWS ignores the very real harms that delaying performance would inflict on Microsoft. AWS sat by for three months as Microsoft and DoD invested heavily in preparations to perform the JEDI contract. Now, just two weeks before DoD's long-announced "go live" date, AWS seeks to stop that progress in its tracks. A preliminary injunction would dissuade top-tier engineers from signing on to the stalled project, sap the momentum that Microsoft's efforts have generated among DoD agencies and commands, and disrupt the orderly ramp-up and transition that Microsoft and DoD have been orchestrating over the past three months.

Finally, the national security harms to DoD—and to the public interest—strongly disfavor an injunction. AWS's self-serving suggestion that halting the JEDI project would be harmless because DoD can continue to use its patchwork of existing cloud services contracts ignores the fundamental purpose of the JEDI project, which is to harness the extraordinary capabilities of a unified, enterprise-level cloud infrastructure to achieve critical national security objectives. The public interest lies in ensuring our Armed Forces are equipped with the best technology, as quickly as possible, to best defend the Nation. AWS previously told this Court just that. The public interest is not served by granting AWS's belated request for preliminary relief. The motion should be denied.

[redacted]

QUESTION PRESENTED

Whether AWS is entitled to the extraordinary relief of a temporary restraining order or preliminary injunction.

STATEMENT OF THE CASE

In October 2019, DoD awarded Microsoft the JEDI contract after a rigorous examination in which it concluded that Microsoft's Azure solution would provide the best product at the best price. Since that award, Microsoft and DoD have dedicated themselves to the complex and costly preparatory activities required to launch JEDI in accordance with DoD's timelines. AWS's motion for preliminary relief seeks to disrupt that work and delay the orderly resolution of this case.

A. DoD's Cloud Computing Priorities and the JEDI Procurement

The rapid, secure transfer of information is of paramount importance to our Nation's security and to the effective operation of the Armed Forces. DoD has determined that its existing computing infrastructure is "too federated, too slow, and too uncoordinated to enable the military to rapidly use DoD's vast information to make critical, data driven decisions." Tab 241, AR60089. Indeed, even where individual DoD agencies are using cloud services, users do not necessarily "have timely access to cloud computing resources that are flexible to mission needs," Tab 17, AR324, and DoD lacks "a coordinated enterprise-level approach to cloud infrastructure," Tab 7, AR178.

For that reason, in September 2017, DoD announced its intention to acquire a "modern enterprise cloud services solution" that would leverage "pioneering technologies" in the commercial space while remaining secure enough to host unclassified, secret, and top secret

[redacted]

information.[1] In particular, DoD sought "technical parity with [the] commercial cloud" in order to ensure that its cloud infrastructure would be continuously updated and would afford DoD all of the benefits of commercial innovation. Tab 89, AR5936.

DoD also made clear that its goal was "for the JEDI Cloud acquisition vehicle to be accessible to all users throughout every organization [in] the Department."[2] In other words, the goal of the JEDI contract was not merely to provide cloud services to individual segments of DoD, but rather to provide one, unified vehicle for adoption of cloud infrastructure and platform services that would "provide data exchange across all classification levels and DoD components, to include intelligence and mission partners," Tab 17, AR321, and that would "seamlessly extend[] from home front to the tactical edge," *id.* AR324.

B. Microsoft's Commercial Cloud Solution

Microsoft is one of the world's leading software and technology companies. Its state-of-the-art commercial cloud solution, Azure, serves the needs of America's largest and most successful corporations. Tab 485, AR179142. Azure is superior to other cloud products along a number of axes, including its [redacted]

Because of Microsoft's superb reputation and Azure's unique benefits, 90 percent of Fortune 500 companies use Azure. *Id.* AR179142-43. Those Microsoft customers entrust Microsoft with their most challenging cloud computing requirements. For example, Microsoft has

[1] *See* U.S. Dep't of Defense, *Accelerating Enterprise Cloud Adoption* (Sept. 13, 2017) https://www.nextgov.com/media/gbc/docs/pdfs_edit/090518cloud2ng.pdf.

[2] U.S. Dep't of Defense, *Accelerating Enterprise Cloud Adoption* (Feb. 15, 2018), https://www.defense.gov/Newsroom/Releases/Release/Article/1442705/accelerating-enterprise-cloud-adoption/.

[redacted]

partnered with Chevron to modernize oil field operations and bring cloud computing technology to some of the harshest and most remote operating environments on earth. *Id.* AR179143. Companies like Walmart, Bank of America, Coca-Cola, and BP have likewise chosen Microsoft's commercial Azure infrastructure as their go-to cloud platform. *Id.* The requirements and objectives of these companies drive continuous competition and innovation in Microsoft's technology. *Id.* AR179143-44. And Microsoft's commercial cloud offering is also available internationally, in 140 different countries and 56 regions. *Id.* AR179142. Microsoft is thus uniquely prepared to satisfy DoD's cloud computing requirements across the globe, simply by offering parity with its Azure commercial cloud offering. *Id.* AR179143.

Microsoft's dominance in cloud computing extends well beyond the commercial space. Azure has been serving the public sector for decades, including 7,000 federal, state and local agencies, from the FBI to the Department of Veterans Affairs. *Id.* AR179142-43. Most importantly, however, Microsoft has served DoD itself through a 40-year partnership. *Id.* AR179139. Azure provides the Department of Defense Information Network with protected, dedicated routes to serve deployed forces. *Id.* AR178143. And in September 2018, Microsoft began providing the Air Force with network services through Azure's "wide area network" (WAN)—the largest global WAN of any cloud provider—which enables access to DoD data for mobile and remote users. *Id.* Microsoft's years of experience serving both commercial and public-sector customers made it a natural fit for the JEDI Cloud procurement.

C. DoD Selects Microsoft's Less Expensive, Technically Superior Cloud Computing Solution

In July 2018, DoD issued its final Request for Proposals for the JEDI contract. *See* Tab 1, AR1-97. In addition to certain "gate" criteria to be considered at the first phase of the procurement,

[redacted]

the RFP enumerated seven evaluation factors, as follows, and identified their relative importance (*see generally* Tab 1, AR88-95):

- Factor 2: Logical Isolation and Secure Data Transfer.
- Factor 3: Tactical Edge Devices.
- Factor 4: Information Security and Access Controls.
- Factor 5: Application and Data Hosting and Portability.
- Factor 6: Management and TO 001.
- Factor 7: Small Business Participation.
- Factor 8: Demonstration.

Each offeror was also required to give an overall description of its pricing proposal and to provide prices for specific scenarios detailed in the RFP. Tab 1, AR83-85.

Microsoft, AWS, Oracle, and IBM submitted initial proposals in response to DoD's RFP. Microsoft's proposal centered on adapting its commercial cloud solution, Azure, to the special needs of a large government organization like DoD. *See* Tab 196a, AR54003. Unlike its competitors, Azure integrates seamlessly with an organization's existing software—including Microsoft's popular Windows operating system and suite of Office products—and is uniquely equipped to offer "hybrid" solutions that blend existing on-premises capabilities with cloud-based computing functions. *Id.*

In April 2019, DoD announced that only Microsoft and AWS had satisfied the RFP's gateway criteria. Tab 457, AR176398. In May 2019, following DoD's discussions with AWS and Microsoft, DoD issued Amendment 0005 to the RFP. *Id.*; Tab 338, AR151400. That amendment clarified that, for purposes of the price scenarios, offerors should assume that all data be "highly accessible" [redacted] Tab 302, AR64310. DoD later further clarified that "highly accessible" meant "online and replicated storage." Tab 304, AR64332. On September 5, 2019, both offerors submitted their final revised proposals (FRPs) to DoD. AWS's price was [redacted] higher than Microsoft's total price of $678 million. Compl. ¶ 108.

[redacted]

After a careful analysis, the Source Selection Advisory Committee's (SSAC) report recommended that the contract be awarded to Microsoft. Tab 457, AR176406. The report gave both proposals [redacted]. *Id.* AR176398-99. But the SSAC concluded that Microsoft's report was "superior" as to Factors 5 and 6—and thus "significantly superior" as to overall non-price factors. *Id.* AR176404, 176406. As to the price factor, the SSAC agreed with the Price Evaluation Board (PEB) that the offerors' price assessments were accurate and complete, *id.* AR176404, and concluded that Microsoft's proposal was [redacted] less expensive. As noted above, Microsoft's total evaluated price was more than [redacted] less than AWS's total price. *Id.* AR176405. Because Microsoft offered DoD a superior product at a better price, the SSAC recommended awarding the JEDI contract to Microsoft. *Id.* AR176406.

On October 17, 2019, the Source Selection Authority (SSA), [redacted], accepted the SSAC's recommendation and awarded the JEDI contract to Microsoft. In so doing, she echoed the SSAC's findings that Microsoft was [redacted] to AWS in terms of Factors 5 and 6, as well as "superior" as to price. Tab 459, AR176415-17. DoD informed Microsoft and AWS of the SSA's award decision on October 25, 2019. Compl. ¶ 188.

D. Microsoft and DoD Expend Substantial Resources to Prepare for Performance of the Contract

After the award, DoD and Microsoft immediately began preparatory activities, with substantive performance of the JEDI contract to begin on February 11, 2020. Given the magnitude of the project, these activities have required a massive effort across a variety of dimensions, from recruiting and personnel management, to technical development, to subcontracting efforts. All in all, Microsoft has committed [redacted] over the past three months in anticipation of the February 2020 launch of JEDI. Decl. of Vice President of Microsoft Azure, Thomas Keane ¶ 6 (*see* Appendix, Exhibit 1 ("Keane Decl.")).

[redacted]

In particular, Microsoft began the process of recruiting and hiring [redacted] of technical software and hardware engineers to meet anticipated demand for the JEDI Cloud. *Id.* ¶ 7. Microsoft ultimately expects to hire [redacted] engineering and technical management positions over the next year, [redacted] Microsoft also engaged [redacted] Decl. of Microsoft's General Manager, Timothy Turitto ¶ 7 (*see* Appendix, Exhibit 2 ("Turitto Decl.")).

In December 2019, Microsoft hosted a major kickoff event in Washington, D.C. in order to prepare DoD agencies and personnel to quickly adopt JEDI and to ensure adequate adoption of the program. *Id.* ¶ 5. Microsoft invested [redacted] in the event to generate buy-in and momentum toward the shared goal of robust adoption of JEDI in February. *Id.*

E. AWS Files This Bid Protest, Raising Belated Challenges to the Solicitation and Unfounded Allegations of Bias

On November 22, AWS filed its complaint in this bid protest alleging—for the very first time—assorted defects in the JEDI Cloud procurement process. Although DoD made clear that it was proceeding with preparatory activities in advance of a full deployment of JEDI on February 11, AWS chose not to seek any form of preliminary injunctive relief at that time.

AWS's complaint asserts seven counts. Counts I and II allege various technical errors in the procurement, expressing disagreement with DoD's determination that Microsoft's offering is superior and represents the best value for the government. Compl. ¶¶ 192-209. Count III challenges the express terms of the solicitation itself, including DoD's decision not to include "past performance" as an evaluation factor as well as the requirements clarified by Amendment 0005. *Id.* ¶¶ 23-24, 210-14. Count IV claims that the errors alleged in Counts I, II, and III cumulatively led to an irrational decision as to which proposal represented the best value for DoD. *Id.* ¶¶ 215-

[redacted]

18. And finally, Counts V through VII allege that the JEDI Cloud procurement was biased against AWS, based largely on public statements and tweets by President Trump critical of AWS's parent company (Amazon) and its CEO (Jeffrey Bezos). *Id.* ¶¶ 219-234.

ARGUMENT

An "injunction is a drastic and extraordinary remedy, which should not be granted as a matter of course." *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 165 (2010) (citation omitted). A preliminary injunction "may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008). In deciding whether to grant preliminary injunctive relief, courts consider four factors: (1) whether the plaintiff is likely to prevail on the merits; (2) whether the plaintiff will suffer irreparable harm if the Court withholds injunctive relief; (3) whether the balance of hardships favors the grant of injunctive relief; and (4) whether granting such relief would serve the public interest. *Id.* at 20.

For purposes of this motion, AWS has abandoned its allegations in Count III and its bias and conflict of interest allegations in Counts V, VI, and VII. And for good reason: They are waived under *Blue & Gold Fleet, L.P. v. United States*, 492 F.3d 1308 (Fed. Cir. 2007), as Microsoft has established in its motion to dismiss. *See* ECF 133 (Jan. 24, 2020). Those counts also lack substantive merit, as there is no evidence DoD's technical and procurement experts were influenced—in any way—by President Trump's statements about Amazon or Mr. Bezos.

As a result, AWS's request for preliminary relief rests entirely on Counts I, II, and IV, which raise a grab-bag of technical disagreements with the DoD experts who conducted the procurement. But AWS cannot show a likelihood of success on any of these counts, and the equitable factors strongly disfavor halting JEDI implementation. The motion should be denied.

[redacted]

I. AWS IS NOT LIKELY TO SUCCEED ON THE MERITS

"[A] movant is not entitled to a preliminary injunction if he fails to demonstrate a likelihood of success on the merits." *Nat'l Steel Car, Ltd. v. Canadian Pacific Ry., Ltd.*, 357 F.3d 1319, 1325 (Fed. Cir. 2004) (citation and footnote omitted)). To prevail in a bid protest, a plaintiff must show that the challenged agency action was "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). Under that highly deferential standard, a procurement decision may be set aside only if it "lacked a rational basis" or if the agency's decision-making involved "a clear and prejudicial violation of applicable statutes or regulations." *Impresa Construzioni Geom. Domenico Garufi v. United States*, 238 F.3d 1324, 1332-33 (Fed. Cir. 2001) (citation omitted).

Challenges involving "the minutiae of the procurement process in such matters as technical ratings . . . involve discretionary determinations of procurement officials that a court will not second guess." *E.W. Bliss Co. v. United States*, 77 F.3d 445, 449 (Fed. Cir. 1996); *Galen Med. Assocs., Inc. v. United States*, 369 F.3d 1324, 1339 (Fed. Cir. 2004) (describing an agency's technical evaluation of proposals as "an inherently judgmental process requiring deference."). "[R]eviewing courts [must] give the greatest deference possible to [] determinations on technical matters, in recognition of the special expertise of procurement officials." *AM Gen., LLC v. United States*, 115 Fed. Cl. 653, 677 (2014) (Campbell-Smith, J.). Here, AWS shows no likelihood of success on the merits on any of its technical challenges.

A. DoD Properly Evaluated Price Scenario 6 Under Factors 5 and 9

AWS's primary merits argument challenges DoD's assessment of Factor 5, which addressed the offerors' approach to the data hosting and portability requirements of the RFP, and DoD's assessment of Factor 9, which addressed the offeror's price. *See* ECF 130-1, at 15-22.

[redacted]

Specifically, AWS disputes DoD's technical assessment and price evaluation regarding Price Scenario 6, which required offerors to propose a technical solution to the specific scenario (to be evaluated by the Technical Evaluation Board (TEB)) and a price for that specific solution (to be evaluated by the PEB). AWS complains that DoD's evaluation did not take into account the particular type of storage proposed by Microsoft for this scenario and that DoD should have increased Microsoft's price. *Id.* AWS's complaint is meritless because (1) it proposed the same type of storage to satisfy Price Scenario 6, and (2) Microsoft's solution fully complies with the terms of the RFP.

1. AWS, Like Microsoft, Proposed [redacted] Storage for Price Scenario 6

AWS notes that all data in Price Scenario 6 had to be "highly accessible," which meant "online and replicated storage." ECF 130-1, at 15-22 (quoting Tab 304, AR64332 (Q&A IPR006)). AWS alleges that, contrary to these requirements, Microsoft proposed [redacted] storage [redacted] which AWS contends should have resulted in Microsoft being eliminated from the competition. *Id.* at 20-22. According to AWS, had Microsoft actually proposed the [redacted] storage allegedly required, Microsoft's price would have increased by [redacted]. *Id.* But AWS fails to tell the court that ***AWS also proposed*** [redacted] ***storage*** for Price Scenario 6. *See, e.g.,* Tab 378, AR155003 (discussing use of [redacted]). AWS also expressly told DoD that [redacted] storage was [redacted] (*id.*), which AWS asserts meets the requirements of Price Scenario 6. There is no basis for AWS to complain about a storage solution it also proposed and which it has asserted satisfies the RFP's requirements.

The specific type of storage that AWS proposed to satisfy the same requirements of Price Scenario 6 about which AWS complains was [redacted] *See* Tab

[redacted]

378, AR155003, 155008-09. AWS's proposal identifies its [redacted] Tab 367, AR152664 (emphasis added). In AWS's priced Basis of Estimate for Price Scenario 6, AWS discusses its storage components for the scenario as expressly including [redacted] *See* Tab 378, AR155008. Figures 9 and 10 on the pages that follow show [redacted] (*id.*), confirming the earlier statement at *id.* AR155003. AWS also provided DoD with details regarding its pricing for [redacted] for Price Scenario 6. *See id.* AR155030.[3]

AWS's use of its [redacted] storage technology [redacted] for this portion of Price Scenario 6 is functionally no different from Microsoft's proposal, [redacted]. *See* Tab 412, AR 173697-98 (technical solution for Price Scenario 6); Tab 425, AR 175215 (price proposal for Price Scenario 6). Indeed, AWS told DoD that [redacted] Tab 378, AR155011 (emphasis added). So contrary to its litigation position, in its proposal AWS was clear that [redacted] storage was [redacted] and actually used it in its proposed solution for Price Scenario 6.

2. Microsoft's Proposal Met the Requirements of the RFP

Microsoft's proposed solution to Price Scenario 6 meets the RFP's requirement for "highly accessible" storage. For part of its solution, Microsoft proposed [redacted] Tab 425, AR175215. Microsoft's proposal states that [redacted]

[3] [redacted] *See* Tab 367, AR152745.

[redacted]

[redacted] Tab 408, AR173458. There is [redacted] *See id*. AR173459. Where the RFP's definition for online storage requires that data be "immediately accessible" (Tab 29, AR650), Microsoft's proposal of [redacted] satisfies this technical requirement. Microsoft's proposed solution using its [redacted] solution therefore satisfies the RFP's definition of "highly accessible" storage, and thus also meets the requirements for "online" storage under the RFP, regardless of the commercial labels that both parties used as part of their solutions.[4]

AWS also attempts to draw a thin distinction between [redacted] AWS's Factor 5 proposal for Price Scenario 6 [redacted] *See* Tab 371, AR152866; *compare also id*. *with* Tab 412, AR173698. AWS ignores that its argument is premised upon the defined term "highly *accessible*," while Price Scenario 6 actually refers to the data in that scenario as "highly *available*," an undefined term. ECF 130-1, at 17-20; Tab 302, AR64310, 64327. AWS completely avoids this distinction, instead assuming without explanation that this term simply means the same as "highly accessible" and "online" storage. *See* ECF 130-1, at 18 ("Price Scenario 6 repeatedly stated that data should be 'highly available'—i.e.,

[4] AWS's proposal similarly states that the [redacted] storage it proposed for Scenario 6 [redacted] Tab 367, AR152666.

[redacted]

stored Online"). Microsoft's proposal fully recognized this distinction and provided a technically acceptable solution. *See* Tab 412, AR173697-98.

3. AWS's Argument Is Untethered to Any RFP Requirement

AWS's challenge also fails because it provides no explanation as to how DoD's evaluation of the technical feasibility of Price Scenario 6 deviated from the RFP's stated requirements regarding how DoD would conduct this evaluation. It is blackletter law that this Court may not second guess the discretionary determinations of procurement officials on "minutiae of the procurement process in such matters as technical ratings." *COMINT Sys. Corp. v. United States*, 700 F.3d 1377, 1384 (Fed. Cir 2012). The Court thus does not "evaluate the proposal anew, but instead will examine the agency's evaluation to ensure that it was reasonable and in accord with the evaluation criteria listed in the solicitation." *Textron, Inc. v. United States*, 74 Fed. Cl. 277, 286 (2006). AWS claims that the evaluation of the TEB was unreasonable for failing to disqualify Microsoft over this purported storage issue (ECF 130-1, at 19), but AWS's argument is completely untethered to the evaluation criteria in the RFP. No provision of the RFP requires such a result, and AWS tellingly points to none.

The RFP explained that, as one component of many for the evaluation of Factor 5, DoD would evaluate "the degree to which the technical approach and Unpriced [Basis of Estimate] evidence a technically feasible approach when considering the application and data hosting requirements in Section L for this Factor and the specific scenario requirements in Attachment L-2." Tab 301, AR64304. There is no disqualification mechanism associated with this evaluation criteria in the RFP, nor are there any criteria stating specifically that DoD would evaluate the type of storage being proposed. *Id.*

[redacted]

As required by the RFP, DoD assessed Microsoft's proposed solution for Price Scenario 6 as part of its overall evaluation of Factor 5. *See* Tab 332. In this evaluation, DoD described Microsoft's technical proposal for Price Scenario 6 and concluded that the solution was a "technically feasible approach." *Id.* AR151328. The evaluation of this portion of Microsoft's proposal goes into extensive detail regarding what specifically Microsoft proposed and how those elements would work together to provide the solution. *Id.* AR151327-28. DoD even described how Microsoft's solution would meet DoD's storage requirements, including its provisions for [redacted] *Id.* AR151328. AWS entirely ignores the extensive evaluation that DoD actually conducted to assess the technical feasibility of Microsoft's proposal for Price Scenario 6, including Microsoft's storage solutions.

4. AWS Suffered No Prejudice from Microsoft's Reliance on [redacted] Storage

Even if Microsoft had improperly proposed [redacted] storage as part of its solution and AWS had not, neither of which is the case, AWS cannot demonstrate prejudice because Microsoft's solution to Price Scenario 6 would only have increased by approximately [redacted] and AWS's solution would still have been much more expensive than Microsoft's solution. AWS erroneously claims that Microsoft gained a [redacted] price advantage by proposing [redacted] storage. But this claim is specious because this figure is merely the total difference in the price of storage between AWS's and Microsoft's solutions to Price Scenario 6. Much of the price differential between Microsoft and AWS in Price Scenario 6 is actually attributable to Microsoft's decision to use a discount strategy that resulted in [redacted] decrease in price." Tab 455, AR176363. In contrast, AWS proposed [redacted], and thus its price is extremely high. *See* Tab 380, AR155354-56 [redacted]

[redacted]

AWS's claim regarding a purported [redacted] price advantage fails to account for Microsoft's discounts, [redacted] *See generally* Tab 416, AR173845 [redacted] Using Microsoft's proposed pricing for online storage would only increase Microsoft's price by [redacted] after taking the applicable discounts (which AWS ignores) into account.

This difference in price is straightforward to calculate because offerors proposed storage prices by the Gigabyte, as required by the RFP. *See, e.g.* Tab 425, AR175215 [redacted]; Tab 378, AR155030 [redacted]. There is thus a common basis to evaluate pricing, even if changing the type of storage from [redacted] to online storage. Performing this (unnecessary) change to the price results in a much lower price impact than AWS claims.

[redacted]

AWS also ignores that its price would also have to increase under its own erroneous theory, because it also proposed [redacted] storage as discussed above.[7] Thus, even taking into account

---

5 [redacted]

6 [redacted]

7 [redacted]

[redacted]

recalculated amounts, AWS's proposal would still be much more expensive than Microsoft's proposal. AWS thus cannot demonstrate prejudice.

B. DoD Properly Evaluated the Factor 8 Demonstrations

AWS devotes a major section of its argument to challenging DoD's assessment of Microsoft's in-person demonstration of its capabilities under Factor 8. *See* ECF 130-1, at 8-9, 16, 22-31, 52-53. But AWS misunderstands the purpose of the Factor 8 demonstrations and their accompanying procedures. That purpose was to confirm each offeror's general capabilities—not, as AWS would have it, to require the offeror to satisfy a specific and detailed set of performance metrics that do not appear in either the RFP or the testing procedures.[8] DoD reasonably concluded that Microsoft's performance in the demonstrations satisfied the RFP's generally stated capability requirements.

1. The Evaluators Reasonably Concluded that Microsoft Successfully Completed Scenario 8.2 of the Demonstration

During the second test scenario, DoD tested the ability of an offeror's cloud system to elastically respond to incoming requests and recover from a decrease in healthy servers able to respond to such requests. *See* Tab 287, AR64173-75. AWS claims [redacted]

[8] Unlike the other technical factors, there are no specific elements tied to Factor 8 in either Section L or M of the Solicitation. Section M explains only that Factor 8 "will evaluate the extent to which the scenarios are successfully demonstrated using the proposed approach for Factor 1 through 6." Tab 301, AR64305. The timing of the Factor 8 demonstrations also demonstrates that they were not the equivalent of a comprehensive acceptance test with detailed specifications, as AWS asserts. They were run two times, once in April 2019 and then repeated in May 2019, after neither offeror passed the first round. *See* Tabs 307, 308. That was before the parties submitted either their Interim or Final Proposal Price Revisions, June 12 and September 5, 2019 respectively. *See* Tabs 309-22 and Tabs 344-438. They also occurred prior to the completion of discussions between the government and the offerors. *See* Tab 343 (discussions continuing through August 2019).

[redacted]

[redacted] ECF 130-1, at 23-25. AWS's claims mischaracterize the demonstration procedures and results.

AWS first asserts that Microsoft [redacted] *Id.* at 3, 24-25. Scenario 8.2 was a scaling exercise to "demonstrate the creation and configuration of an automatically scaling pool of virtual machines through their Graphical User Interface (GUI)." Tab 287, AR64173. To that end, the demonstration procedures noted that a successful implementation of Scenario 8.2 would "create a dynamically created pool of compute resources to respond to incoming requests from a client." *Id.* Essentially, the offeror was to show that as requests increased, the number of servers ("nodes") available to respond to those requests would also increase; as the number of requests decreased, the number of available servers would also decrease. *Id.* DoD set a minimum and maximum number of healthy servers, and deployed an application that would randomly destroy healthy servers and require them to be removed from the pool of available servers. *Id.* AR64174. Thus, Scenario 8.2 tested both the ramp-up and ramp-down of servers, and the ability of the offeror's system to recover from events that unexpectedly reduced the pool of virtual machines.

The procedures provided that DoD would simulate a certain number of requests per second for set periods of time, each of which was designated a "phase." *Id.* There would be four phases, the first three of which would ramp up requests while the fourth would decrease the number of requests. *Id.* At the end of each phase, DoD evaluators would count the number of healthy responding servers. *Id.* When all phases were complete, a final count would be taken after a cooldown period of four minutes. *Id.* AR64175.

[redacted]

The TEB Report for each offeror recorded the number of active servers at the end of each phase. Tab 307, AR64391; Tab 308, AR64414. But the numbers that the TEB recorded in its Report captured only the number of active servers available at the exact moment when the number was recorded. It did not indicate the number of active servers available *throughout* each load test and did not reflect the number of servers which were available even seconds before or after the recorded number. DoD has consistently taken the sensible approach that the single digit readings do not tell the whole story of Scenario 8.2. As the TEB Report states in reference to the evaluation of the first demonstration, [redacted] Tab 308, AR64412.

The information available to the evaluators while the scenario ran and the log records of the demonstration collected at the end of this scenario show the number of available servers throughout each of the load testing periods. *See* Tab 287, AR64188 (requiring output from the second scenario of "[a]ny log files available from the global cloud (audit logs, API logs, scaling resource logs, etc.)"); Tab 291 at 2:03:00-2:05-03 (showing that Microsoft [redacted]). The evaluators were able to review the full ability of the systems to respond to an increase and decrease in the number of servers, as appropriate, throughout the exercise to determine whether each offeror successfully demonstrated scaling. *See, e.g.*, Tab 308, AR64415 (confirming Microsoft's [redacted]). The video logs available to the evaluators showed that [redacted]. *See* Tab 291 at 1:50:40-1:51:45 (explaining that [redacted]). The evaluators reasonably found that Microsoft demonstrated the capability for scaling

[redacted]

based on all the information it received *continuously* during the demonstration, instead of focusing only on individual snapshot readings taken at the end of each phase.[9]

Relying again upon the single-moment end-of-phase numbers, AWS also claims that Microsoft [redacted] ECF 130-1, at 25. The numbers recorded in the TEB Report for both offerors are just snapshots of the exact number of nodes available at the moment the count is taken. Tab 287, AR64174. DoD was running an application to have healthy nodes destruct at random intervals, and required those servers to be removed, in order to test a system's ability to recover quickly if active servers failed at an unexpectedly rapid rate. *See id.* AR64186-87 (explaining that servers should be shut down after two failed health checks). This, in addition to the 100-node cap on active servers, made it difficult for offerors to maintain any particular availability of healthy servers at every second. Given that it takes a few seconds to create new servers, it was always possible that at any given moment, the [redacted] *See* Tab 295 at 1:12:42.

[9] AWS repeatedly points to language in the instructions for Scenario 8.2 expecting that the number of compute nodes would "seamlessly" increase and decrease in response to changes in demand. ECF 130-1, at 24-25; Tab 287, AR64186. But the instructions did not define "seamlessly," and AWS has no basis for overriding DoD's practical application of that term in the circumstances here. A too literal reading of "seamlessly" makes no sense, given that between each phase there was a gap while the number of active nodes was recorded and issues were clarified before moving on to the next phase of node testing. *See, e.g.*, Tab 291 at 1:50:45-1:58:18 (showing a small gap between the end of phase 3 and the beginning of phase 4). It is therefore not surprising that there may be some adjustment in the scaling between phases. [redacted]

[redacted]

AWS's claim that Microsoft should have [redacted] for Scenario 8.2 (ECF 130-1, at 25) misrepresents the actual results of the demonstration and the stated standard for determining whether a test was successful. DoD retained broad discretion regarding how it would evaluate the demonstrations, explaining to offerors in the RFP that DoD would "evaluate the extent to which the scenarios are successfully demonstrated using the proposed approach for Factor 1 through 6." Tab 301, AR64305. Indeed, the RFP does not prescribe or even reference the [redacted] grade that AWS asks this Court to apply, and AWS provides no citation for its suggestion. DoD reasonably concluded Microsoft and AWS met the requirements of Scenario 8.2 to "[d]emonstrate an automatically scaling pool of virtual machines." Tab 287, AR64186; *see* Tab 307, AR64392; Tab 308, AR64414.

2. The Evaluators Reasonably Concluded that Microsoft Successfully Completed Scenario 8.3 of the Demonstration

In Scenario 8.3, DoD tested the ability to utilize the tactical edge (TE) device in "tactical environments." Tab 287, AR64175. AWS claims that Microsoft [redacted] —in its tactical edge solution during Scenario 8.3." ECF 130-1, at 29. Under the demonstration procedures, a "successful implementation" of the scenario would demonstrate that applications could "save data to the Offeror's TE device in spite of network disconnect/reconnect, being physically dropped, and exposed to environmental factors, while opportunistically syncing that data to Offeror's cloud environment." Tab 287, AR64175. [redacted]

AWS makes much of a [redacted] ECF 130-1, at 29; *see also* Tab 291 at 3:34:10-3:42:27. But AWS fails to mention that DoD was unable to identify the

[redacted]

[redacted] *See, e.g.*, Tab 291 at 1:29:56-1:32:29 [redacted]

After the [redacted] *See* Tab 291 at 3:42:00. That was entirely appropriate: [redacted] Tab 287, AR64178 (emphasis added). Microsoft's [redacted] was thus fully consistent with DoD's procedures.

3. The Evaluators Reasonably Concluded that Microsoft Successfully Completed Scenario 8.4 of the Demonstration

During Scenario 8.4, which tested security, offerors were required to "demonstrate that the security controls and user Access Control Lists (ACLs) work as expected, and audit logs are generated during the course of any access, security, and API events . . . both through the GUI as well as interactively via a command line interface (CLI)." Tab 287, AR64178. AWS claims that Microsoft's performance did not satisfy the demonstration protocols in various ways, and, therefore, that Microsoft should have been found unacceptable. ECF 130-1, at 26-28. But again, AWS misconstrues the purpose of the demonstrations. This is an area where application of the rigid standards that AWS would impose on Microsoft would mean that AWS would *also* have failed the demonstration.

First, AWS alleges that under Step 2 of the test procedures, Microsoft [redacted] *Id.* at 26. The procedures for Scenario 8.4 focused on issuing identities using a token,

[redacted]

allowing access to cloud services based on a federated confirmation system, time-limiting that access, and revoking access as needed. Tab 287, AR64178-81. DoD broadly defined a "token" as "a general term for: access token, access key, assertion, claim, **or other form of user authorization**." *Id.* AR64179 (emphasis added). Several tokens were to be generated, assigned characteristics, utilized, and revoked throughout the scenario. *Id.*

DoD's broad definition of "token" encompassed [redacted] AWS used a [redacted] Tab 370, AR152845. Microsoft, [redacted] Tab 411, AR173674-75. It used [redacted] Tab 291 at 4:18:30-4:39:30. Specifically, it employed [redacted] *See id.* This [redacted] Tab 287, AR64179.

Step 2 of the test procedures required generating a token for a user, limiting the amount of access time provided by that token to five minutes, logging into the portal with that token, and watching the token expire and access be revoked. Tab 287, AR64192-93. AWS claims that Microsoft [redacted] ECF 130-1, at 26-27. But AWS's focus on [redacted] ignores the demonstration procedure's specific recognition that a "token" includes other forms of user authorization. Microsoft's [redacted] fully conformed with the requirements of the demonstration.

[redacted]

Microsoft also used [redacted] in the section of the demonstration showing configuration of access to data and services, Scenario 8.4, Step 2. Tab 287, AR64192-93. The specific order of the steps of this section of the demonstration, designed for a traditional access token, needed to be [redacted]. Microsoft explained that [redacted] *See* Tab 291 at 4:19:54, 4:34:15-19.

Contrary to AWS's claim (ECF 130-1, at 26), DoD did not [redacted]. Rather, the evaluators explained that they were looking for [redacted] Tab 291 at 4:33:00-4:33:54. Microsoft did just that, using its [redacted] Tab 291 at 4:21:00-30, 4:34:47-4:45:05. Microsoft's use of [redacted] Tab 308, AR64423.[10]

[10] AWS also incorrectly claims that Microsoft did not [redacted] *See* ECF No. 130-1, at 27. The demonstration procedures call for revoking the user's "token via GUI" and then attempting to log in with the token (which should fail). Tab 287, AR064193. As described above, however, Microsoft's [redacted] Instead, Microsoft demonstrated it could [redacted] (Tab 291 at 4:45:07-4:48:17), [redacted] While Microsoft did not [redacted] *See* Tab 291 at 4:48:17. AWS's claim that this is [redacted] is belied by the evaluators [redacted] Tab 308, AR64423.

[redacted]

Second, Step 3 of the demonstration procedures for Scenario 8.4 required the offerors to demonstrate security controls. Tab 287, AR64193. One of the controls tested was the ability to tag objects and only allow access based on those tags. *See id.* AWS claims that Microsoft [redacted] ECF 130-1, at 27. Microsoft explained during its demonstration that [redacted] Tab 291 at 4:59:01-5:04:54. AWS makes much of this, although the DoD evaluators at the time of the demonstration, *see id.*, and in the TEB Report, *see* Tab 308, AR 64422-23, properly recognized that this [redacted] Microsoft [redacted]. Tab 291 at 4:59:01-5:04:54; *see also* Tab 287, AR64193. DoD thus reasonably concluded Microsoft was [redacted]

Even if Microsoft's approach [redacted]. For example, Step 2 of the procedures for Scenario 8.3 required the offerors to demonstrate the ability to "[e]nable access based on policies" and set a policy to only allow tokens to last for five minutes, or whatever minimum number is possible. Tab 287, AR64192. But AWS's demonstration video indicates that [redacted] *See* Tab 295 at 4:22:48. [redacted]. Rather, to accomplish these goals, the customer [redacted] *Id.*;

[redacted]

id. at 4:24:00-4:24:12. Nonetheless, DoD allowed this [redacted] Tab 307, AR64401.

Third, Scenario 8.4's demonstration procedures indicated that a "successful implementation" would include that audit logs be "generated during the course of any access, security, and API events during the course of this exercise." Tab 287, AR64178. AWS claims that Microsoft [redacted] *See* ECF 130-1, at 28. Again AWS is wrong.

The "Output" section of the demonstration procedures for Scenario 8.4 provided that the offeror was to provide "[a]ll access, security and API logs." Tab 287, AR64181. In response to that requirement, Microsoft [redacted] *See* Tab 291 at 5:08:37-5:23:25. [redacted] *Id.* Microsoft subsequently [redacted] *Id.*

AWS points to the evaluators' note that [redacted] and concludes that Microsoft had [redacted]. Tab 308, AR64423; ECF 130-1, at 28. But the demonstration procedures for Scenario 8.4 do not [redacted] *See* Tab 287, AR64191-94. Based on Microsoft's demonstrated ability to [redacted] the evaluators had every reason to believe that Microsoft had the [redacted]. And that conclusion, derived from Microsoft's demonstrated

[redacted]

capability in [redacted] was reasonably confirmed by Microsoft's [redacted].[11]

C. DoD Reasonably Evaluated the Tactical Edge Devices Under Factor 3

Under Factor 3, the offerors were required to propose "tactical edge compute and storage capabilities across the range of military operations that balance ***portability*** with ***capability***." Tab 342, AR151494 (emphasis added). DoD placed "far greater emphasis" on the evaluation of ***existing*** solutions already in production and gave "lesser weight" to proposed future capabilities available after award. *Id.* AR151505. As to portability, the RFP's only requirement was that Category One devices "should not require heavy equipment to move." *Id.* AR151494. The RFP did not contain any size or weight limitations for the proposed devices, nor did it prescribe minimum computing or storage capabilities.

The offerors proposed different solutions to balance the requirements of portability and capability. Microsoft generally proposed [redacted] while AWS proposed [redacted] AWS claims that its devices are superior merely because [redacted] (ECF 130-1, at 32-33), but this contention ignores that [redacted] is just one aspect of the Factor 3 evaluation. As depicted in the tables below, Microsoft's devices are [redacted]

[11] AWS repeats its baseless claim that DoD should have graded Microsoft [redacted] and again fails to cite to any evaluation criteria or other RFP requirement that would require this outcome. As explained above, there are no such requirements.

[12] Tab 369, AR152811, AR152817; Tab 410, AR173640. AWS proposed [redacted] For purposes of comparison, the table above reflects the [redacted]

[redacted]

[redacted]

DoD rigorously evaluated the offerors' devices and rationally concluded that [redacted] Tab 456, AR176375. Moreover, the SSAC [redacted] Tab 457, AR176401. In the end, the SSA reasonably adopted the SSAC's findings. Tab 459, AR176416.

---

[13] Tab 369, AR152805; Tab 410, AR173641, AR173643.

[14] An FPGA, or field-programmable gate array, is a component used to build reconfigurable digital circuits. The TEB correctly recognized [redacted] ab 330, AR151280.

[redacted]

1. DoD Equally Evaluated the Offerors' Tactical Edge Devices as to Portability and Support for Dismounted Operations

AWS argues that "DoD [redacted] with respect to portability and dismounted operations that Microsoft's [redacted] devices inexplicably did not receive." ECF 130-1, at 32. AWS is mistaken.

The TEB reasonably evaluated the offerors' proposals to determine whether they proposed an existing device that was portable by a single individual and, thus, capable of dismounted operations. Ultimately, [redacted] Although AWS complains that the TEB did not [redacted] this had no impact on the evaluation or final award decision and did not result in any prejudice to AWS.

The TEB clearly found that Microsoft's [redacted] *Id.* AR151290. Likewise, the SSAC determined that Microsoft [redacted] Tab 457, AR176401. The SSA adopted the SSAC's evaluation. Tab 459, AR176413. Thus, even if the TEB had [redacted] this would not have changed the SSA's decision.

At best for AWS, the absence of a [redacted]

[redacted]

[redacted] that does not come close to "proving that a significant error marred the procurement in question." *Land Shark Shredding, LLC v. United States*, 142 Fed. Cl. 301, 305 (2019) (Campbell-Smith, J.). Regardless of the TEB's analysis of specific strengths and weaknesses, the record is clear that the SSA made the final award based on the SSAC's conclusion that [redacted] AWS's disparate treatment claim is meritless.

2. DoD Rationally [redacted]

AWS disagrees with the TEB's decision to [redacted] Tab 324, AR151169, AR151171; *see* ECF 130-1, at 33-35. That challenge is nothing more than a disagreement with DoD's "highly discretionary technical evaluation of proposals." *Voith Hydro, Inc. v. United States*, 143 Fed. Cl. 201, 214 (2019) (Campbell-Smith, J.).

Unlike AWS, Microsoft proposed to use [redacted] *See* Tab 410, AR173641-43. The TEB reasonably concluded that Microsoft's solution [redacted] 330, AR151283. By contrast, the TEB [redacted] Tab 324, AR151169.

AWS argues that DoD applied an unstated criterion to its proposal because the RFP did not specifically require the offerors to [redacted] ECF 130-1, at 33-35. But the RFP clearly announced how DoD would evaluate the offerors' proposals to

[redacted]

meet the [redacted] Tab 342, AR151494 (emphasis added). [redacted] it was reasonable for DoD to consider whether the offerors proposed [redacted] Microsoft's device can [redacted] By contrast, AWS's device and [redacted] DoD reasonably exercised its technical judgment and concluded that Microsoft's [redacted] solution would be most advantageous to warfighters at the tactical edge. *See AM Gen., LLC*, 115 Fed. Cl. at 677.

3. DoD Correctly Concluded that [redacted]

AWS argues that the SSAC improperly found that it [redacted] ECF 130-1, at 35-37. That mischaracterizes the record.

The SSAC's conclusion was appropriately focused on both offerors' ***existing*** devices, which were to receive "far greater emphasis" in the evaluation under the RFP's express terms. Tab 342, AR151505. The SSAC reasonably determined that, [redacted] Tab 457, AR176401-02. The SSAC's statement [redacted] *See* Tab 324, AR15166 [redacted]; Tab 330, AR151279

[redacted]

[redacted]

Nevertheless, AWS argues that the SSAC's conclusion is inconsistent with the TEB's evaluation. According to AWS, [redacted] ECF 130-1, at 36. AWS is wrong: The TEB clearly found that the [redacted] *See* Tab 324, AR15166. AWS concedes that a [redacted] *Id.* The TEB quite rationally concluded that AWS's [redacted] *Id.*

In fact, the record shows that Microsoft's [redacted] *See* Tab 369, AR152805; Tab 410, AR173643. In light of [redacted] it is hardly surprising that AWS's own proposal concedes that [redacted] Tab 369, AR152805 (emphasis added).

AWS also claims that the SSAC did not properly recognize the portability of its [redacted]

[15] AWS's [redacted] *See* Tab 369, AR152804. In contrast, Microsoft's [redacted] *See* Tab 410, AR173642.

[redacted]

[redacted] but this argument ignores that the SSAC [redacted] Tab 457, AR176401. Moreover, as discussed above, the SSAC's statement with respect to portability specifically addressed the offerors' [redacted] Tab 324, AR151167. Nevertheless, the TEB [redacted] s (*id.* AR151170) and the SSEB [redacted] Tab 456, AR178375. The SSAC adopted these findings and specifically acknowledged the [redacted] Tab 457, AR176401-02. The TEB and SSAC evaluations of the [redacted] device are fully consistent.

4. Both Offerors Proposed [redacted] for Dismounted Operations and DoD Reasonably Evaluated AWS's [redacted]

AWS next argues that "DoD's evaluation of the [redacted] was unreasonable." ECF 130-1, at 37-38. As an initial matter, AWS is wrong that the [redacted] *Id.* at 37. Microsoft proposed a [redacted] Tab 410, AR173647 (emphasis added). Like the [redacted] proposed by AWS, Microsoft's [redacted] *Id.* The SSAC reasonably focused [redacted] Tab 457, AR176402. AWS's view that the [redacted] should have received more

[redacted]

credit merely second-guesses the SSA's technical judgment.

AWS also disputes the SSEB's observation that [redacted] Tab 456, AR176376. But AWS proposed [redacted] *See* Tab 369, AR152811. AWS offered [redacted] whereas Microsoft proposed [redacted] *Id.*; *see also* Tab 410, AR173640. The SSEB recognized that, [redacted] In any event, as AWS concedes, the SSEB fully acknowledged [redacted] Tab 456, AR176376. The SSAC considered these differing viewpoints and reasonably determined that AWS's [redacted] *See* Tab 457, AR176401.

5. DoD Reasonably Evaluated the Offerors' Battery Solutions

AWS also misrepresents the record with respect to DoD's evaluation of the offerors' competing battery solutions for their Category One devices. *See* ECF 130-1, at 39-40. The RFP does not contain any minimum requirement for battery runtime. Rather, it merely states that the device must have "[t]he ability to be powered by battery." Tab 342, AR151494. AWS's initial proposal [redacted] Tab 208, AR57972; *see also* Tab 195a, AR25476 [redacted] In doing so, the TEB explained the basic reason for the battery power requirement: [redacted] Tab 208,

[redacted]

AR57972. The TEB did not state or imply anything about the importance of battery ***runtime***—it was simply [redacted] *Id.* [redacted] *See* Tab 209, AR57991; Tab 330, AR151288.

AWS is wrong to claim there was an improper "shift in the importance of battery power" during the evaluation. ECF 130-1, at 39. [redacted] Tab 324, AR151174-75; Tab 330, AR151288-89. Still, AWS argues that DoD [redacted] ECF 130-1, at 39. But DoD observed Microsoft's [redacted] *Compare* Tab 209, AR57991 *with* Tab 330, AR151288. The record thus disproves AWS's allegation of disparate treatment. In evaluating Microsoft's [redacted] Tab 330, AR151288.

Finally, AWS boldly asserts that its "battery power capabilities are [redacted] than Microsoft's." ECF 130-1, at 40. It supports this claim with a grossly misleading apples-to-oranges comparison of devices that [redacted]. AWS specifically [redacted] A more apt comparison is Microsoft's [redacted] Unlike the [redacted] As shown below, AWS's battery is [redacted] than Microsoft's and yet Microsoft's battery

[redacted]

achieves [redacted]

[redacted]

See Tab 369, AR152805; Tab 410, AR173643 [redacted]; *id.* AR173645. There is no basis to second-guess DoD's reasonable evaluation of the offerors' battery solutions.

D. DoD Reasonably Evaluated AWS's Hypervisor Solution and Third-Party Marketplace Offerings

AWS claims that DoD discounted the benefits of its hypervisor solution, and the extent of its third-party marketplace offerings. These are mere disagreements with DoD's expert technical evaluations, and with respect to hypervisors, an untimely challenge to the JEDI ground rules.

1. DoD Reasonably Evaluated the Offerors' Hypervisor Solutions

The RFP's parameters were broad and gave no special weight to hypervisor security. *See* Tab 1, AR77-97. AWS claims that under Factor 2, the SSAC improperly discounted the superiority of AWS's hardware-based Nitro hypervisor solution, downplayed the importance of [redacted], and gave insufficient weight to [redacted]. ECF 130-1, at 43. With respect to Factor 4, AWS claims that DoD did not properly recognize the benefits of the Nitro architecture with respect to information security. *Id.* at 45-46.

The problem for AWS is that the RFP did not place that much importance on the evaluation of hypervisor technology. This technology is mentioned in just one of four subfactors under

[redacted]

Factor 2, and there, hypervisor is only one among eight *sub*-subfactors to be evaluated. *See* Tab 1, AR78-79. It is not even mentioned in Factor 4 at all. *Id.* AR80-81. AWS's criticism regarding the importance that DoD should have placed on hypervisor technology is a belated attempt to rewrite the RFP, and that challenge is untimely. *See Blue & Gold Fleet, L.P. v. United States*, 492 F.3d 1308 (Fed. Cir. 2007). Moreover, as explained below, DoD's findings on both factors were reasonable and supported by the record.

Factor 2. Contrary to AWS's assertions, the SSAC recognized Nitro's [redacted] and agreed with the SSEB that Nitro [redacted] in ways that [redacted] Tab 457, AR176400-01. The SSAC further agreed that [redacted] *Id.* AR176400.

While recognizing Nitro's value with respect to logical isolation, the SSAC concluded that [redacted]. The SSAC explained that [redacted] *Id.* AR176401. Far from [redacted], ECF 130-1, at 43, the SSAC merely recognized that based on [redacted] the SSAC [redacted] Tab 457, AR176400. The SSAC took nothing away from the TEB's and SSEB's evaluations of AWS's Nitro solution [redacted]. Rather, the SSAC rationally balanced the advantages of each proposal [redacted]

[redacted]

[redacted]. AWS offers no citations or evidence indicating that this conclusion was somehow irrational or unsupported by the record. *See Banknote Corp. of Am., Inc. v. United States*, 56 Fed. Cl. 377, 384 (2003), *aff'd*, 365 F.3d 1345 (Fed. Cir. 2004).

Moreover, AWS's claim about Nitro's alleged superiority is based on the erroneous assertion that Azure relies on [redacted] Microsoft's Azure solution uses [redacted] *See, e.g.*, Tab 408, AR173280; Tab 409, AR173612. The TEB correctly understood this. *See* Tab 329, AR151247 (noting [redacted] (emphasis added).

AWS exaggerates the extent to which its Nitro solution relies on [redacted] By its own account, Nitro is a [redacted] *See* Tab 368, AR152764-65 (noting that the [redacted] AWS also touts the use of [redacted]" ECF 130-1, at 44, while it disregards Microsoft's [redacted] at Tab 411, AR173660-61.

AWS implies bad faith by arguing that the SSAC [redacted] ECF 130-1, at 44. AWS points to its proposed [redacted]

[redacted]

[redacted] *Id.* at 44-45. AWS acknowledges, however, that [redacted] *Id.* at 44, n.19; *see also* Tab 368, AR152797. DoD's decision not to assign a strength for a [redacted] was squarely within its discretion. *See E.W. Bliss Co.*, 77 F.3d at 449. The same discretion is owed to the SSAC's decision to credit Microsoft's [redacted] Tab 457, AR176401. AWS fails to show why the perceived benefits of Microsoft's [redacted] were irrational.[16]

AWS claims its hypervisor should have received extra credit under Factor 2, but it has presented no evidence that undermines the SSAC's conclusion—echoed by the SSA—that while there were [redacted], neither was technically superior to the other overall. Tab 457, AR176400; Tab 459, AR176413-16.

Factor 4. AWS claims that "DoD failed to recognize key features that AWS's Nitro architecture provides to deliver the highest level of information security currently possible." ECF 130-1, at 45. AWS discusses what it perceives to be the merits of its hypervisor solution, but does

[16] AWS argues that [redacted] ECF 130-1, at 44 n.19. Microsoft's [redacted] In any event, DoD had broad discretion to determine that Microsoft's proposed [redacted] Similarly, the TEB noted that [redacted] Tab 323, AR151122.

[redacted]

not cite to any specific Factor 4 criterion or explain how DoD improperly evaluated its proposal against those criteria. This is not surprising: Factor 4 required offerors to propose their approach to security *management* for the cloud, beyond the baked-in security of the underlying cloud infrastructure. As such, Factor 4 ***does not mention*** the hypervisor. Tab 1, AR80-81. But even to the extent that AWS suggests its hypervisor supports information security, AWS's proposal undercuts its own claims regarding Nitro's so-called feature of "eliminating" administrator access to cloud environments. ECF 130-1, at 46. AWS's proposal states that it is "[redacted] Tab 370, AR152834.

Also, as it does elsewhere, AWS merely seeks extra credit for certain features of its proposal. But here as there, technical evaluation judgments are properly left to DoD's discretion. *See E.W. Bliss Co.*, 77 F.3d at 449. For instance, AWS points to its approach to supply chain integrity, including [redacted] and its "proprietary, automated patching technology." ECF 130-1, at 46. But AWS's proposal is not superior to Microsoft's in either area. *See, e.g.*, Tab 411, AR173661-62 [redacted]; Tab 331, AR151297-98 [redacted]. AWS has identified nothing in the record showing that DoD's evaluation of its hypervisor solution was irrational or improper.

2. DoD Reasonably Evaluated AWS's Third-Party Marketplace Offerings

AWS next argues that its third-party marketplace was a significant advantage over Microsoft, and that DoD incorrectly determined that [redacted] AWS's third-party marketplace

[redacted]

offerings were not available at the time of award by misreading its proposal. ECF 130-1, at 47. But AWS revised its price proposal to say [redacted] Tab 309, AR67032; Tab 384 ([redacted] supports the SSAC's conclusion that [redacted] AWS third-party marketplace offerings were [redacted] in the JEDI Cloud. This language indicates that—as the SSAC [redacted] Tab 457, AR 176403.

More importantly, because AWS [redacted] AWS now claims that when it [redacted] ECF 130-1, at 48, but it is AWS's burden to submit an adequately written proposal. *See, e.g., Westech Int'l, Inc. v. United States*, 79 Fed. Cl. 272, 296 (2007). In any event, there is no explanation why offerings that [redacted] and there is nothing irrational in DoD's interpretation of this language, or in its conclusion that this was a [redacted]

AWS further claims that it [redacted] "to comply with DoD's instructions during discussions." ECF 130-1, at 48. AWS appears to suggest that DoD indicated its [redacted] *Id.* at 48-49. To support this argument, AWS does not cite to any of the discussion

[redacted]

materials in the record, but instead cites to the PEB's summary of changes to the price catalog, which does not indicate that DoD instructed AWS to change its proposal. *Id.* (citing Tab 455, AR176356). Nothing in the record shows that AWS was instructed that its [redacted], and that requirement appears nowhere in the RFP. *See* Tab 2, AR100-01, 105. AWS also baldly claims that, rather than instruct Microsoft that its third-party catalog [redacted], DoD simply "*assumed* that Microsoft's third-party offerings [redacted]" and were available at award. ECF 130-1, at 49 (emphasis added). But there was no assumption. Microsoft's offerings are available immediately upon award, [redacted]. To the extent the confusion on this issue stems from AWS's mistaken view that [redacted], it is not DoD's (or Microsoft's) fault and does not justify overturning the award. The SSAC's analysis of AWS's proposal was entirely proper.

E. AWS's Remaining Challenges to the Evaluation Process Fail

AWS concludes its motion with a grab-bag of alleged errors that DoD supposedly made when evaluating its proposal. *See* ECF 130-1, at 50-55. None of these claims have merit.

1. AWS Was Not Entitled to the Strengths It Claims for Factors 2 and 5

As to Factor 2, AWS cites four strengths and one risk reduction that DoD identified in its February 19, 2019 evaluation of AWS's initial proposal but "inexplicably omitted" from its evaluation of AWS's final proposal. *See* ECF 130-1, at 51. Contrary to AWS's claims, the absence of each alleged strength from DoD's final evaluation is easily explained and properly subject to DoD's discretionary expert judgment. *See Metropolitan Interpreters and Translators, Inc. v. United States*, 145 Fed. Cl. 495, 511 (2019) (Campbell-Smith, J.) ("[C]hallenges to the SSA's

[redacted]

judgment in assigning—or not assigning—various strengths to [a] proposal fall squarely within the realm of minutiae into which the court must not intrude.").

First, AWS argues that DoD failed to assign it a strength for [redacted] ECF 130-1, at 51 (citing Tab 206, AR57906). But DoD fully credited AWS on this point: It explicitly granted AWS a "**strength**" for [redacted] Tab 323, AR151130. To be sure, DoD phrased this strength slightly differently than in its initial evaluation. *See* Tab 206, AR57906 [redacted] But this difference is hardly surprising, given that AWS's initial proposal offered [redacted] *Compare* Tab 206, AR57906 *with* Tab 323, AR151129 [redacted] Substantively, the two strengths are the same.

Second, AWS claims it was denied a strength for its "cryptographic protections for disk storage and network traffic in hardware." ECF 130-1, at 51 (citing Tab 206, AR57906-07). But Microsoft's proposal offered the very same protections, and it was also denied a strength. *See* Tab 409, AR173603-08 (detailing Microsoft's [redacted]. AWS therefore suffered no prejudice from DoD's decision not to assign it this strength, because if DoD had assigned it to AWS, it would have had to assign a corresponding strength to Microsoft.

[redacted]

Third, AWS complains it was denied a strength for its "marketplace offerings." ECF 130-1, at 51 (citing Tab 206, AR57924). But again, Microsoft's proposal contained similar marketplace offerings, and Microsoft did not receive a strength. *Compare* Tab 409, AR173622 [redacted] *with* Tab 206, AR57924 n.152 [redacted] DoD's decision not to assess a strength for this feature left the two offerors on equal footing.

Fourth, AWS claims it was also entitled to a strength for its CloudFormation service. ECF 130-1, at 51 (citing Tab 206, AR57924). According to AWS, CloudFormation [redacted] Tab 368, AR152776. But once again, Microsoft also proposed [redacted], and it was not assigned a strength either. *See, e.g.*, Tab 408, AR173215 ([redacted] AWS suffered no prejudice from DoD's evenhanded assessment.

Finally, AWS complains that it was erroneously denied a risk reduction that it originally received because its "network design and implementation have been reviewed, audited, and accredited at the Secret and Top Secret levels which eases JEDI Cloud adoption." ECF 130-1, at 51; Tab 206, AR57915. But this accreditation pertained specifically to the [redacted] built for the [redacted], not for DoD. Thus, as AWS later admitted in its final proposal, the accreditation merely represented "[redacted]. Tab 368, AR152768. DoD's ultimate decision to remove this risk reduction was reasonable. *See* Tab 323, AR151141-42.

[redacted]

As to Factor 5, AWS cites three additional strengths that it claims were improperly excluded from DoD's final evaluation after being included in its January 11, 2019 initial evaluation. Specifically, AWS points to: (1) its proposed [redacted] (2) its plan to use [redacted]; and (3) the "matur[ity]" of its marketplace. ECF 130-1, at 50-52 (citing Tab 212, AR58033-36). But once again, Microsoft's proposal had identical or superior Factor 5 offerings, and it was not assigned strengths for those offerings, either. *See generally* Tab 332 (Microsoft Factor 5 evaluation assigns no strengths in these areas). As to the [redacted], Microsoft proposed to [redacted]. *Compare* Tab 371, AR152846 *with* Tab 412, AR173679 (discussing Microsoft [redacted]. Microsoft [redacted] *See* Tab 412, AR173679. And the basis for the strength that was initially assigned for AWS's marketplace offering—that it [redacted] (*see* Tab 212, AR58035)—was [redacted] *See* Tab 412, AR173678-79 (discussing [redacted]). DoD's evaluation of these factors reveals no disparate treatment.

2. AWS Was Not Entitled to the Strengths It Claims for Factor 8

AWS also complains that it exceeded DoD's requirements in the Factor 8 demonstrations in several ways that should have been, but were not, recognized as strengths. *See* ECF 130-1, at 52-53. Specifically, AWS challenges DoD's failure to grant strengths for exceeding the

[redacted]

performance metrics on Scenarios 8.1 and 8.3 and for the number of cloud services it ran on its tactical edge device in Scenario 8.3. *Id.*

But Microsoft [redacted] *See* Tab 308, AR644409, 644417. And because the point of the demonstrations was simply to accomplish the scenarios' stated objectives—whether with two services or twenty—it is irrelevant that [redacted] *See generally* Tab 287 (demonstration procedures do not require the use of more than one service). Thus, the evaluators reasonably exercised their discretion in not awarding AWS a strength as to Factor 8.

3. DoD Reasonably Evaluated the Offerors' Management Approaches Under Factor 6

AWS also contends that DoD erred in its evaluation of Factor 6, by (1) evaluating a prior version of AWS's proposal; (2) incorrectly concluding that AWS had not [redacted]; and (3) ignoring AWS's tested management approach. ECF 130-1, at 53-55.

AWS's first objection has no basis in the record. Despite being told otherwise, AWS insists that DoD evaluated the wrong version of its proposal, apparently because DoD stated that AWS [redacted] ECF 130-1, at 54 (citing Tab 327, AR151216). AWS emphasizes that in its FPR, it stated [redacted] *Id.* at 53-54. But the lack of an express reference to AWS's [redacted] provides no reason to believe DoD evaluated a prior version of AWS's proposal. In fact, DoD made clear in its response to AWS's debrief questions that it evaluated the proper version of AWS's proposal. *See* Tab 491, AR180080. This is confirmed by other areas of AWS's evaluation for Factor 6: DoD's initial evaluation found that

[redacted]

[redacted]. *Compare* Tab 215, AR58079 (Initial Evaluation) *with* Tab 327, AR151222 (IPR Evaluation) *and* Tab 451, AR176331 (FPR adopting findings of IPR Evaluation). And the decision to assign strengths is firmly within the evaluators' discretion. DoD was not required to give AWS extra credit where it was satisfied that AWS [redacted]. Tab 301, AR064286.

AWS is also wrong to complain that DoD failed to recognize that it [redacted] and then relied on that incorrect conclusion [redacted]. ECF 130-1, at 54 (citing Tab 457, AR176403). The SSAC identified three reasons why [redacted]: (1) [redacted] Tab 457, AR176403. By contrast, "AWS offered (a) [redacted] *Id.* AWS completely misses a critical difference between AWS and Microsoft that the SSAC specifically and undeniably recognized regarding these services: Microsoft offered [redacted] and AWS did not. Irrespective of whether there was parity between the offerors' [redacted] offerings, AWS did [redacted] and the SSAC therefore concluded [redacted] Tab 457, AR176403.

Although AWS asserts that it too offered [redacted], ECF 130-1, at 54, DoD could reasonably conclude that AWS's offerings would [redacted] because [redacted]

[redacted]

[redacted]—a mistake of AWS's own making. AWS's reference to [redacted]. *See* Tab 375, AR154073. DoD was not obligated to consider AWS's [redacted] In fact, AWS's discussion of its [redacted]. *See e.g.*, Tab 372, AR152878 (noting that AWS [redacted]). By contrast, Microsoft clearly stated in its Factor 6 Proposal that it was offering DoD [redacted] Tab 408, AR173400. Further, AWS offered *only* [redacted] Tab 375, AR154083, whereas DoD had requested [redacted]. Tab 27, AR618 ("[redacted]."). For all these reasons, DoD could have reasonably concluded that [redacted]

AWS also claims that the SSAC misconstrued its [redacted] offerings by failing to observe that its offering was [redacted]. ECF 130-1, at 54. However, this misses the mark of the TEB's evaluation. Rather than distinguishing Microsoft's offering [redacted].[17] AWS fails to explain how its [redacted] as described in AWS's Factor 6 Proposal, measure up to Microsoft's [redacted] Beyond indicating that [redacted]

[17] Even if DoD was concerned with price, AWS's lack of clarity in its Factor 6 proposal is a mistake of AWS's own making.

[redacted]

[redacted]. *See* Tab 367, AR152619 [redacted]), AR152694 [redacted] Tab 372, AR152878-79 [redacted] It is also not clear that these [redacted] provide any additional support beyond that which is necessary to meet the contract's requirements.

By contrast, Microsoft's [redacted] Tab 413, AR173719. These [redacted] *Id.* [redacted] *Id.* The TEB properly identified this as a strength. Microsoft's [redacted] play a very different role from AWS's [redacted]. *See* Tab 372, AR152878. DoD properly differentiated the offerors on this basis.

Finally, AWS contends that Microsoft cannot be rated higher [redacted] ECF 130-1, at 55. But as Microsoft's Factor 6 Proposal shows, Microsoft has extensive experience helping more than 200,000 organizations transition to the cloud, including enterprise-level transitions in the private and public sectors. Tab 413, AR173706. Microsoft has cultivated a strong relationship with DoD, and has worked on a number of cloud projects with DoD in the course of their forty-year partnership. *Id.* Microsoft has also implemented the management strategy proposed for JEDI in numerous other projects, including with DoD. *Id.* AR173707. Moreover, AWS's past management experience in projects with the

[redacted]

[redacted] is largely irrelevant to implementation of the JEDI contract: The RFP explicitly *rejected* the approach taken by [redacted] in favor of a commercial cloud approach. Tab 161, AR22854 (noting that because [redacted] believed that commercial clouds were less secure, it opted for a less commercial approach); Tab 27, AR608 (identifying commercial parity as a key pillar of the JEDI cloud).

Ultimately, Microsoft proposed a comprehensive and detailed approach to meeting DoD's Factor 6 requirements and ensuring success on the contract. *See* Tab 408; Tab 413. This included providing [redacted] Tab 413, AR173716, AR173400, AR173719. For these reasons, DoD reasonably concluded that Microsoft proposed a superior solution that more directly met the JEDI contract requirements.[18]

II. AWS WILL NOT SUFFER IRREPARABLE HARM ABSENT AN INJUNCTION

As with the likelihood of success on the merits, "a movant cannot be granted a preliminary injunction unless it establishes" irreparable harm. *Amazon.com, Inc. v. Barnesandnoble.com, Inc.*, 239 F.3d 1343, 1350 (Fed. Cir. 2001). AWS has not come close to satisfying that independent requirement here, for at least three reasons.

First, AWS waited nearly three months to seek a preliminary injunction, even though it was well aware of DoD's intention to implement the contract on February 11, 2020. *See* ECF 130-1, at 55. Such delay cuts strongly against a finding that AWS's alleged harm warrants injunctive

[18] In a buried footnote near the end of its brief, AWS raises a litany of meritless arguments, accompanied by a series of misleading string citations to the administrative record. ECF 130-1, at 50 n.20. These allegations are not developed in any way in AWS's motion and contain nothing more than the same disagreement with assigned strengths and weaknesses.

[redacted]

relief. In *Facility Services Management, Inc. v. United States*, for example, this Court held that a plaintiff's motion for emergency relief was "untimely" where the plaintiff was notified that the government intended to "phase-in [the] intervenor-defendant's performance," and the plaintiff initially indicated it would not seek a preliminary injunction. 140 Fed. Cl. 323, 326 (2018) (Campbell-Smith, J.). The Court explained that even if new documents in the administrative record had changed the plaintiff's mind, the plaintiff had waited "more than three weeks" after the filing of the administrative record to seek emergency relief. *Id.*; *see also Elmendorf Support Services Joint Venture v. United States*, 105 Fed. Cl. 203, 210 (2012) ("Equity aids the vigilant, not those who slumber on their rights."). The court made a similar point in *Software Testing Solutions, Inc. v. United States*, 58 Fed. Cl. 533 (2003), noting that the "failure to act sooner undercuts the sense of urgency that ordinarily accompanies a motion for preliminary relief and suggests that there is, in fact, no irreparable injury." *Id.* at 537 (citation omitted).

Here, rather than act promptly to enjoin DoD from proceeding with the contract, AWS waited a month after the contract was awarded to file its complaint, and then another two months to file this motion. Because of AWS's delay, Microsoft has been forced to respond to AWS's motion in just over a week, and more importantly, AWS has placed this Court in the position of resolving its request in less than two weeks. There is no reason to indulge AWS's delay.

Second, and in any event, the harms AWS purports to identify do not flow from DoD's decision to begin implementing JEDI in mid-February, instead of after AWS's bid protest is resolved. Rather, they flow from the mere fact that AWS was not the successful bidder. AWS contends that it "could lose the opportunity to perform the JEDI Contract, earn the revenue and profits resulting from contract performance, ensure its technology is widely used by DoD, and gain additional experience working with the Government." ECF 130-1, at 57. But those "alleged harms

[redacted]

result not from a lack of opportunity to compete for the contract, but from loss of the actual contract." *Sierra Military Health Servs. v. United States*, 58 Fed. Cl. 573, 582 (2003).

The law is clear: Where a plaintiff cannot show that "it will lose the opportunity to compete for the contract in question if the court does not grant some form of temporary injunctive relief," it cannot establish irreparable harm. *GEO Grp., Inc. v. United States*, 100 Fed. Cl. 223, 228 (2011); *see also Sierra,* 58 Fed. Cl. at 582 (no irreparable harm where the protestor "[would] still have the opportunity to obtain the contract" if its protest were sustained); *Land Shark Shredding, LLC*, 142 Fed. Cl. at 312 (explaining that if the protester were to prevail in its protest, "an orderly transition to a new contract award would mitigate any harm" from the absence of a preliminary injunction); *Found. Health Fed. Servs. v. United States*, No. 93-1717NHJ, 1993 WL 738426 (D.D.C. Sept. 23, 1993) (rejecting argument that awardee would become so entrenched during transition that protestor would be irreparably harmed absent an injunction). To be sure, a preliminary injunction may be appropriate where a contract "is for the purchase of items or the construction of a building" and "continued performance during the protest period could produce a *fait accompli*." *Sierra*, 58 Fed. Cl. at 584. But contracts for continuing services—like the JEDI contract here—do not pose the same problem because they are ongoing, and their performance during the pendency of a bid protest does not deprive the protestor of the full value of the original contract in the event of a recompete. *Id.* (no irreparable harm in context of heath care services contract).

AWS's argument to the contrary relies entirely on cases involving *permanent* injunctions, where the court had already determined that the protester had prevailed on the merits and would be *permanently* deprived of the opportunity to compete for the contract absent injunctive relief. *See* ECF 130-1, at 57 (citing *FCN, Inc. v. United States*, 115 Fed. Cl. 335, 338 (2014); *Palladian Partners, Inc. v. United States*, 119 Fed. Cl. 417, 458-59 (2014); *HP Enter. Servs. LLC v. United*

[redacted]

States, 104 Fed. Cl. 230, 245 (2012); *Heritage of Am., LLC v. United States*, 77 Fed. Cl. 66, 78 (2007)). Those cases say nothing about harms that would result from the denial of a *preliminary* injunction.

AWS also points to *Cigna Government Services, LLC v. United States*, 70 Fed. Cl. 100 (2006). There, the court held that an agency's decision to override the automatic stay triggered by a GAO bid protest under the Competition in Contracting Act was arbitrary and capricious in part because the agency failed to consider the harm to the protestor. But the court did not apply an "irreparable harm" standard, and it looked to the unique circumstances of the solicitation. In particular, the transition to the awardee required the protestor—who was the incumbent contractor—to transfer its processes and methodologies to the new awardee and could therefore confer an "unfair competitive advantage" on the awardee in a recompete. *Id.* at 102, 109.

No such special considerations apply here. As AWS itself points out (ECF 130-1, at 58-59), AWS already has cloud contracts with DoD, and therefore has substantial contact with the agency, making it highly unlikely that Microsoft will somehow obtain a "competitive advantage" from its performance over the next several months. AWS likewise fails to explain how Microsoft could possibly use "non-public information" (ECF 130-1, at 58) learned during performance to its competitive advantage in the unlikely event that DoD requests revised proposals in any recompete. AWS's allegations appear to presume that—in the event of a recompete—DoD would fail to put out a fair Request for Proposals and would instead permit Microsoft to benefit from "non-public information." ECF 130-1, at 58. There is no basis for such speculation.

Finally, AWS contends that it has already suffered harm from the JEDI contract because

[redacted]

[redacted]

[redacted] ECF 130-1, at 58-59. Those speculative claims do not establish that AWS will in fact suffer irreparable harm absent a preliminary injunction. Indeed, AWS's long list of existing contracts with DoD strongly suggests DoD will continue to work with AWS across a variety of contract vehicles and will receive any work to which it is entitled, regardless of the JEDI contract. AWS's failure to show irreparable harm is reason enough to deny its motion.

III. AN INJUNCTION WOULD IRREPARABLY HARM MICROSOFT

DoD and Microsoft have been performing the JEDI contract for more than three months. With full knowledge that they would be performing the contract and preparing to onboard customers as early as February 11, 2020, AWS waited nearly 90 days before asking the Court to take the extraordinary step of issuing a temporary restraining order and preliminary injunction. Not only does this delay undercut AWS's claim of irreparable harm, as explained above, but the belated timing of AWS's request inflicts significant harm on Microsoft. As explained below, Microsoft has expended [redacted] to prepare for JEDI's imminent operational date. A preliminary injunction now would cause much more disruption and harm than if the issue had been litigated at the outset of this case last fall. AWS's delay has ensured that the balance of hardships weighs strongly against itself in its request for preliminary relief.

This is precisely the type of harm that courts in the bid-protest context have held will tip the balance in favor of the Government and the winning bidder, where both parties have incurred substantial costs to "ramp up" in preparation for performance of a contract. In *Akal Security v. United States*, for example, the balance of hardships weighed against the protester because the Government had already incurred substantial costs to prepare for its transition to the new contractor, and the successful bidder had "already invested hundreds of thousands of dollars" and

[redacted]

had implemented proprietary systems in preparation for performance of the contract. 87 Fed. Cl. 311, 320 (2009). Similarly, in *Kola Nut Travel, Inc. v. United States*, the court found that the balance of harms favored the defendant and intervenors because they had already begun to implement the relevant contracts and the preliminary injunction would cause "significant disruption and added cost." 68 Fed. Cl. 195, 200 (2005).[19]

Since the JEDI award was announced on October 25, 2019, Microsoft has been performing under DoD's initial Task Order for program management, providing personnel and tools to meet the quality and performance requirements of the contract. The accompanying declarations of Microsoft's General Manager, Timothy Turitto and the Vice President of Microsoft Azure, Thomas Keane explain that Microsoft has invested significant resources to prepare for deployment of the JEDI contract on February 11, 2020, and that a delay in the JEDI contract at this point would cause substantial and irreparable harm to Microsoft.

The JEDI contract represents a massive realignment of DoD's use of technology and computing resources. Microsoft has engaged internal and external resources and devoted significant efforts to make sure personnel and infrastructure are in place to meet and exceed DoD's requirements. *See* Turitto Decl. ¶¶ 7-8; Keane Decl. ¶¶ 6-13. Indeed, Microsoft has committed [redacted] in anticipation of the February 2020

[19] *See also Chenega Healthcare Services, LLC v. United States*, 138 Fed. Cl. 644, 657 (2018) (Campbell-Smith, J.) (holding that government and successful bidder would suffer harm from preliminary injunction due to delays in transition to follow-on contract); *Land Shark Shredding, LLC*, 142 Fed. Cl. at 312 (holding that balance of hardships weighed against preliminary injunction where contract performance had been ongoing for months); *Elmendorf*, 105 Fed. Cl. at 212 (explaining that "[u]ndue delay is relevant in determining the extent to which it has magnified the harm to defendant" and crediting the defendant's assertion that it would suffer far more harm "now than if an injunction had been issued long before [it] began the process" of implementing the challenged contract); *Bannum, Inc. v. United States*, 60 Fed. Cl. 718, 731 (2004) (stating that "a bid protest pressed well into contract performance tips the scale in favor of the awardee").

[redacted]

adoption by DoD agencies of JEDI. Keane Decl. ¶ 6. At this point, DoD customers are about to onboard to JEDI, and Microsoft is ready for them. *Id.* ¶ 5. A preliminary injunction would effectively negate all of the progress Microsoft has made over the past three months of contract performance to prepare for the February 2020 "go live" date. Moreover, it would require Microsoft to maintain its activities, personnel, and resources in a constant state of readiness for full activation of the JEDI contract—at great expense, and with no corresponding compensation. *See* Turitto Decl. ¶¶ 8-9; Keane Decl. ¶¶ 14-20. This is precisely the type of harm that courts consider and seek to avoid when a contract is already in place and moving forward. *See, e.g.*, *Sierra*, 58 Fed. Cl. at 584 (balance of hardships weighed against a preliminary injunction where the awardee's transition work was "complex" and a stay would be disruptive).

One major effort that Microsoft has undertaken over the past three months has been to ramp up recruiting and hiring activities for [redacted] of technical software and hardware engineers (who require security clearances) to meet the anticipated demand for the Azure JEDI Cloud. Keane Decl. ¶¶ 7-16. Because of anticipated demand, the highly technical nature of the services that Microsoft will be providing, and the need for 24/7 on-call support staff to meet the military's needs, [redacted]

[redacted]

Microsoft is now three months into this effort, and a preliminary injunction at this point will harm Microsoft's ongoing efforts to recruit and hire the best personnel for the positions that are necessary to provide support to the JEDI contract. *Id.* ¶¶ 14-17. [redacted] *Id.* ¶¶ 15-17 [redacted] *Id.* ¶ 16. [redacted] *Id.* ¶¶ 15-17. [redacted]. *Id.*

Other efforts that Microsoft has invested in over the past three months of JEDI contract performance will also be wasted if an injunction issues. For example, [redacted]. *See* Turitto Decl. ¶¶ 6-7. Similarly, [redacted] *Id.* ¶ 7. [redacted]s. *Id.*

Microsoft hosted a major kickoff event in Washington, D.C. in December 2019 to prepare DoD agencies and personnel to quickly adopt JEDI and ensure adequate adoption of the program.

[redacted]

Id. ¶ 5. Microsoft invested [redacted] in the event, with the understanding that the resulting momentum and buy-in would result in robust adoption of JEDI in February. *Id.* [redacted] *Id.* ¶ 9. [redacted] *Id.* ¶¶ 9-10. The magnitude of that harm weighs strongly against preliminary injunctive relief.

IV. AN INJUNCTION WOULD HARM THE PUBLIC INTEREST

As DoD explains in its opposition brief, delaying implementation of JEDI will also cause significant harm to the public interest—and, most importantly, to national security. AWS itself acknowledges that the JEDI contract is a "critical defense initiative" that implicates "national security." ECF 130-1, at 59; *see also id.* at 63. This Court should not credit AWS's self-serving contention that *delaying* that critical initiative would be harmless.

Courts adjudicating bid protests must "give due regard to the interests of national defense and national security and the need for expeditious resolution of the action." 28 U.S.C. § 1491(b)(1)(3). For that reason, courts routinely deny preliminary injunctions where they would negatively impact national security. Such concerns are "directly implicated when a procurement involves services critical to the success of military operations" and the safety of our military personnel. *Linc Gov't Servs., LLC v. United States*, 96 Fed. Cl. 672, 702 (2010).[20]

Here, national security interests weigh strongly against granting a preliminary injunction. "Data is one of [DoD's] most valuable strategic asset[s] over the United States' adversaries," and

[20] *See also, e.g., CSE Constr. Co., Inc. v. United States*, 58 Fed. Cl. 230, 263 (2003) (denying injunction where solicitation implicated "military preparedness"); *Aero Corp., S.A. v. United States*, 38 Fed. Cl. 237, 241 (1997) (similar); *Elmendorf*, 105 Fed. Cl. at 212 (similar).

[redacted]

DoD has recognized that its current computing infrastructure is "too federated, too slow, and too uncoordinated to enable the military to rapidly use DoD's vast information to make critical, data driven decisions." Tab 241, AR60089. For that reason, DoD has made JEDI a top priority.

AWS argues that a delay in onboarding customers to the JEDI Cloud is a non-issue because DoD has existing cloud services. ECF 130-1, at 59-60. But AWS's suggestion that DoD use the "more than 600 cloud initiatives across the Department" in lieu of JEDI, *id.* at 59, only underscores DoD's concern that its current technology is "too federated" and "too uncoordinated" to serve our warfighters. The fundamental objective of the JEDI project is not merely to introduce cloud computing to DoD, but rather to provide an integrated, modernized infrastructure that extends to battlefields around the globe and serves agencies and commands across the whole of the Department and across all classification levels. *See supra* at 4. And, as AWS has previously recognized, "DoD has the exclusive right to determine its own needs."[21]

Here, DoD has determined that the JEDI Cloud project is "critical to maintaining our military's technological advantage" and "empower[ing] the warfighter" to win our wars.[22] Accordingly, any delay in widespread adoption of JEDI across DoD would cause substantial harm to a top national security priority.[23] Where, as here, a contract for "services critical to the success

---

[21] AWS's Response To Oracle America, Inc.'s Supplemental Motion For Judgment On The Administrative Record And Cross-Motion For Judgment On The Administrative Record at 1, 25, *Oracle Am., Inc. v. United States*, No. 18-1880C, (Fed. Cl. June 18, 2019), ECF No 88.

[22] U.S. Dep't of Defense, *DoD Cloud Strategy*, Foreword (Dec. 2018), https://media.defense.gov/ 2019/Feb/04/2002085866/-1/-1/1/DOD-cloud-strategy.pdf.

[23] This is a far cry from the non-urgent situations in the cases AWS cites (ECF 130-1, at 57). *See Palantir USG, Inc. v. United States,* 129 Fed. Cl. 218, 294 (2016) (challenging government's *rejection* of a ready technology solution); *Bilfinger Berger AG Sede Secondaria Italiana v. United States*, 97 Fed. Cl. 96, 159 (2010) (rejecting national security justifications for routine property maintenance at DoD facilities); *cf. GTA Containers, Inc. v. United States*, 103 Fed. Cl. 471, 478 (2012) (granting permanent injunction after final determination on merits, but

[redacted]

of military operations," *Linc Gov't Servs.*, 96 Fed. Cl. at 702, has been underway for three months, the balance of hardships and the public interest weigh strongly against AWS's belated request for an injunction.

CONCLUSION

For the reasons set forth above and in DoD's opposition, the Court should deny AWS's motion for a temporary restraining order and preliminary injunction.

Dated: January 31, 2020

Respectfully submitted,

Of Counsel:

LATHAM & WATKINS LLP

Kathryn H. Ruemmler
Abid R. Qureshi
Roman Martinez
Anne W. Robinson
Dean W. Baxtresser
Genevieve Hoffman
Riley Keenan
Margaret Upshaw

555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004
(202) 637-2200 (Telephone)
(202) 637-2201 (Facsimile)

ROGERS JOSEPH O'DONNELL, P.C.

[redacted]

Robert S. Metzger (Attorney of Record)

Jeffery M. Chiow
Neil H. O'Donnell
Lucas T. Hanback
Stephen L. Bacon
Deborah N. Rodin
Cassidy Kim
Eleanor M. Ross

875 15th Street N.W., Suite 725
Washington, D.C. 20005
(202) 777-8952 (Telephone)
(202) 347-8429 (Facsimile)

Attorneys for Intervenor-Defendant, Microsoft Corporation

explaining that court had previously declined to grant a preliminary injunction "in deference to the military's assessment of urgent material needs").

[redacted]